P17742

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

A SYSTEM AND ASSOCIATED METHODS TO DETERMINE AUTHENTICATION PRIORITY BETWEEN DEVICES

Inventor(s):
David Johnston

Prepared by: Michael A. Proksch,
Sr. Patent Attorney

intel®
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR 97124-5961
Phone: (503) 264.3059
Facsimile: (503) 264.1729

Express Mail Label: EV324060228US

EV324060228US

A System and Associated Methods to Determine Authentication Priority Between Devices

Technical Field

[0001] Embodiments of the present invention are generally directed to communication system security and, more particularly to a system and associated methods to determine authentication priority between devices.

Background

[0002] In communication systems, there is often a need or at least a desire to confirm the identity of a remote device with which you are in communication. In fact, many communication system standards will require both parties in communication to authenticate the identity of the other. This level of authentication is typically referred to as two-way, mutual, or bi-directional authentication.

[0003] The conventional approach to performing such mutual authentication requires the use of at least two sequences of messages, the first enabling party A to authenticate party B, and the second enabling party B to authenticate party A. There may be scenarios, however, where one or more of the parties is unwilling to reveal its identity to the other until the other party has first revealed its identity. In such a situation, authentication may never occur and the opportunity for communication lost.

Brief Description of the Drawings

[0004] Embodiments of the present invention are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings in which like reference numerals refer to similar elements and in which:

Fig. 1 is a block diagram of an example communication environment within which the teachings of the present invention may be practiced;

Fig. 2 is a block diagram of an example security agent through which authentication priority may be established, according to but one example embodiment of the invention;

Fig. 3 is a flow chart of an example method for to determine authentication priority, according to but one example embodiment of the present invention;

Fig. 4 is a communication flow diagram exhibiting a method for determining authentication priority according to one example embodiment;

Fig. 5 is a communication flow diagram exhibiting a method for determining authentication priority according to one example embodiment;

Fig. 6 is a communication flow diagram exhibiting a method for determining authentication priority according to one example embodiment; and

Fig. 7 is a block diagram of an example article of manufacture including content which, when accessed by a device, causes the device to implement one or more aspects of one or more embodiment(s) of the invention.

DETAILED DESCRIPTION

[0005] Embodiments of a system and associated methods for determining authentication priority between devices are generally introduced herein. In this regard, according to but one example embodiment of the teachings of the present invention, a security agent is introduced to selectively exchange at least a subset of an authentication policy as a precursor to authentication. The security agent compares at least the received subset of the authentication policy of the

remote device with at least a subset of a local authentication policy to determine a relative authentication priority, i.e., which device must authenticate to the other first.

[0006] Reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases "in one embodiment" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures or characteristics may be combined in any suitable manner in one or more embodiments.

Example Network Environment

[0007] **Fig. 1** illustrates a block diagram of an example communication environment within which embodiments of the present invention may be practiced. In accordance with the illustrated example embodiment of Fig. 1, two or more devices 102 and 104 are depicted in selective communication through one or more wireless communication channel(s) 106. To facilitate such communication, each of the devices 102, 104 are depicted comprising one or more transceiver elements 108, 110, each including at least one transmitter and one receiver, although the invention is not limited in this respect.

[0008] In accordance with the teachings of the present invention, one or more of the devices 102, 104 may include an embodiment of a security agent, e.g., 112 and/or 114, to determine a relative order for authentication between the devices (i.e., an authentication priority). According to one example embodiment, described more fully below, one or more of security agent(s) 112, 114 may exchange at least a subset of an authentication policy with the remote device, compare the

received authentication information (or, subset thereof) against at least a subset of a local authentication policy, and determine which of the device(s) 102, 104 should initiate the actual authentication process based, at least in part, on the result of the comparison. Examples of this determination of authentication priority, and mechanisms for resolving authentication policy conflicts are developed more fully below.

[0009] It will be apparent, given the description to follow, that the innovative security agent may well be implemented in any of a number of alternate embodiments within the scope of the present invention. Example implementations may well include deployment within a transceiver (e.g., agent 114 within transceiver 110), on a network interface card (e.g., within a media access controller (MAC), not particularly illustrated), as a software application within the device (not particularly illustrated), or as a service available to an accessing device (not particularly illustrated), although the scope of the invention is not limited in this regard.

[0010] Those skilled in the art will appreciate that communication environment 100 may well represent any of a number of wired or wireless communication and/or data networks known in the art. In this regard, but for their association with the innovative security agent, device 102 and device 104 are intended to represent any of a wide range of electronic appliances know in the art including, but not limited to wireless communication devices (e.g., cellular telephones, personal communication devices, and the like), computing devices with communications features (e.g., laptops, palmtops, personal digital assistants, desktop computers and the like), network infrastructure equipment (base stations, subscriber stations, hubs, routers, etc.) and the like, or any combination thereof.

[0011] Similarly, but for the possible integration of security agent (see, e.g., 114), transceiver(s) 108 and 110 are intended to represent any of a wide range of transceivers, or disparate

transmitter/receiver pairs known in the art. In this regard, such transceiver(s) may well be comprised of radio frequency transceiver elements, optical transceiver elements, sub-RF electrical transceivers, and the like, or any combination thereof. Similarly, communication channel 106 is intended to represent one or more wireless communication channel(s) established according to the operating parameters and features of the transceiver(s) 108, 110.

[0012] For ease of explanation, and not limitation, an example implementation of the innovative security agent will be developed within the context of a wireless communication system application, although the scope of the invention is not limited in this regard. More particularly, in accordance with but one example implementation, communication environment 100 may represent a wireless metropolitan area network (WMAN) communication environment between a base station (104) and one or more subscriber station(s) 102, in accordance with the developing 802.16 standard within the Institute for Electrical and Electronic Engineers (IEEE). In this regard, the transceiver(s) 108, 110 may represent the transceiver elements (transmitter and/or receiver) necessary to generate a communication channel 106 defined by the emerging 802.16 physical layer (PHY) standard, although the invention is not so limited (see, e.g., IEEE Std 802.**16-2001.** ; IEEE Standard for local and metropolitan area networks; Part 16: Air Interface for Fixed Broadband Wireless Access Systems).

Example Security Agent Architecture

[0013] Fig. 2 illustrates a block diagram of an example security agent architecture 200, in accordance with but one example embodiment of the invention. In accordance with the illustrated example embodiment of Fig. 2, security agent 200 is depicted comprising one or more

of control logic 202, an authentication engine 204, memory 206 and one or more input/output (I/O) interface(s) 208, each coupled as depicted.

[0014] Memory 206 is depicted comprising one or more of security parameter(s) 210, authentication policy/policies 212 and, optionally, one or more applications (e.g., authentication application(s), security application(s), user interface(s), or communication application(s) in support of any of the foregoing) 214. It should be appreciated that security agent 200 may well be implemented in hardware, software, firmware, or any combination thereof. Moreover, although depicted as a number of separate elements, those skilled in the art will appreciate that a security agent of greater or lesser complexity which nonetheless determine the relative priority of authentication prior to actual authentication is anticipated within the scope and spirit of the present invention.

[0015] As used herein, control logic 202 may control the overall operation of the security agent 200. Control logic 202 may selectively invoke instances of authentication engine 204 to determine a relative authentication priority, as described below, in response to internal or external stimuli. In this regard, but for its use in association with the inventive features of security agent 200, control logic 202 is intended to represent any of a wide range of control logic including, but not limited to, microprocessor(s), controller(s), field-programmable gate array(s) (FPGA's), and the like, software to implement such functionality, or combinations thereof.

[0016] Similarly, but for its use in accordance with the example embodiment of security agent 200, memory 206 is intended to represent any of a wide range of storage technology including, but not limited to, volatile memory, non-volatile memory, programmatic memory (e.g., variables, etc.), communication channel memory (e.g., propagated signals, etc.), and the like, although the invention is not limited in this regard. As used herein, security parameters 210 may include one

or more of security settings, security policies, security keys and the like. According to one example embodiment, security parameters 210 include one or more (e.g., three) keys for selective use by security agent 200 in implementing triple data encryption standard (3DES) cryptography of one or more communication messages, although the scope invention is not limited in this regard.

[0017] Input/output (I/O) interface(s) 208 enables one or more elements (202-206) to communicate with external and/or remote elements (e.g., of a host device). According to one example embodiment, security agent 200 may communicate with a local transceiver through such I/O interface(s) 208 to generate, issue and receive one or more messages necessary to determine authentication priority between the security agent and a remote device. In this regard, I/O interface(s) are intended to represent any of a wide variety of wired or wireless communication interfaces known in the art.

[0018] Authentication engine 204 may be selectively invoked by control logic 202 to determine a relative authentication priority between a local device and a remote device. In this regard, authentication engine 204 generates and issues (e.g., through I/O interface(s) 208 and an associated transceiver) one or more messages to the remote device including at least a subset of a local authentication policy. According to one example embodiment, the authentication policy(ies) 212 may be associated with the entire device, or with individual agents/threads within the device.

[0019] The authentication polic(ies) 212 may include content denoting an authentication priority level which denotes whether the local device requires prior authentication of the remote device as a prerequisite to authentication of the local device (i.e., essentially requiring the remote device to reveal its identity first), or not. According to one example embodiment, authentication

priority may be denoted by a single bit: (0) local priority, or (1) remote priority (or, don't care). This authentication priority indicator may well be embedded within a header field, a security field, a payload field, or in a special authentication field of the message (or, datagram) generated for transmission to the remote device. In alternate embodiments, authentication priority designations of greater or lesser complexity may well be used within the scope and spirit of the invention.

[0020] According to one example embodiment, the authentication policy(ies) 212 may also include an indication of device class associated with the issuing device. According to one example embodiment, the indicator of device class (or, significance) may be used to resolve any conflicts in authentication priority levels between the devices (i.e., both devices declare that it has authentication priority over the other). In cases where both authentication policies (local and remote) denote the same authentication priority level, authentication engine 204 may then review the device class indicator associated with the two devices to resolve the conflict. As above, a single bit designator may well be used such as, e.g., (0) for low significance or (1) for high significance, although the invention is not limited in this regard. In certain embodiments, a two-bit field may be used, with one bit associated with the authentication policy and another bit associated with device significance, although the invention is not limited in this regard.

[0021] Upon some internal or external stimuli, security agent 200 may selectively invoke an instance of authentication engine 204 to determine a relative authentication priority between at least two devices – a local device and a remote device. In this regard, authentication engine 204 may generate and issue a message (or datagram) to the remote device including at least a subset of the local authentication policy(ies) 212. As used herein, the internal or external stimuli may include one or more of a periodic or random indication to complete authentication from a host

device, receipt of a message (e.g., broadcast beacon, paging signal, or discovery signal) from a remote device, and the like. The subset of the local authentication policy(ies) 212 may be denoted in any one or more of a header field, security field, authentication field or payload field of the generated datagram (e.g., a packet, word, byte, etc.) transmit from the local device to a remote device through one or more communication channel(s) (in-band and/or out-of-band).

[0022] Authentication engine 204 may also receive a message (or datagram) from a remote device, perhaps in response to a message issued by authentication engine 204, including at least a subset of an authentication policy associated with the remote device. Upon receipt of at least a subset of an authentication policy from the remote device, authentication engine 204 can compare the content of the message against at least a subset of a local authentication policy 212 to determine a relative authentication priority between the devices. According to one embodiment, authentication engine 204 may compare one or more of the indication of authentication priority, and optionally device class, to determine which authentication policy will control subsequent, two-way authentication procedures, i.e., which device will have to initiate authentication disclosing its identity first.

[0023] As used herein, the determination and population of one or more of the authentication information within the authentication policy 212 (e.g., authentication priority, device class, etc.) and/or security parameter(s) 210 may occur in any manner of ways and times. According to one embodiment, the content (210, 212) is determined during manufacture of the device. According to one embodiment, the security parameters 210 may be determined during manufacture, while the authentication policy 212 may be established by an end-user (e.g., an administrator), or vice versa. Any number of permutations of the foregoing are anticipated within the spirit and scope of the present invention.

Example Security Agent Operation

[0024] Having introduced an example embodiment of the architecture and operating environment of the security agent 200, above, attention is now directed to Fig. 3, where a flow chart of an example method for determining the relative authentication priority between two or more devices is presented, in accordance with one example embodiment. For ease of illustration, and not limitation, the method of Fig. 3 is developed with continued reference to Figs. 1 and 2, as appropriate. Nonetheless, it is to be appreciated that the teachings of Fig. 3 may well be implemented in alternate architectures and/or communication environs without deviating from the spirit and scope of the present invention.

[0025] **Fig. 3** is a flow chart of an example method for determining the relative authentication priority of two or more devices, according to one example embodiment of the present invention. In accordance with the illustrated example embodiment of Fig. 3, the method begins with block 302, wherein a first device 102 (e.g., the subscriber station in the WMAN paradigm introduced above) identifies a remote device 104 (e.g., the base station) with which to establish communication. According to one example embodiment, this identification may be the result of receiving a beacon or paging signal from the remote device 104. Alternatively, device 102 may decide to (re)authenticate accessible devices (e.g., 104) from time to time. Regardless of whether the impetus is the result of internal or external stimuli, device 102 invokes an instance of security agent 112 to determine a relative authentication priority between the devices (102, 104) before actual authentication begins.

[0026] In block 304, security agent 112 may selectively initiate the exchange of at least a subset of its authentication policy(ies) 212 with the remote device 104. More specifically, as introduced above, control logic 202 of security agent 112 may invoke an instance of authentication engine 204 to generate and issue a message to the remote device including at least a subset of the authentication policy. According to one example embodiment, the message may include authentication information such as one or more of an authentication priority and/or a device significance associated with device 102. The message, generated by authentication engine 204 is passed to an associated transceiver 108 via I/O interface(s) 208 for transmission to at least the remote device 104.

[0027] In block 306, authentication engine 204 of security agent 112 may compare the authentication information associated with device 104 with local authentication policy information to identify which device (102 or 104) enjoys authentication priority over the other device (i.e., which device must initiate authentication, disclosing its identity first).

[0028] More specifically, according to one example embodiment, authentication engine 204 may receive a response message from the remote device 104 including authentication information (e.g., authentication priority, device class, etc.) associated with at least a subset of the authentication policy 212 of the remote device 104. Authentication engine 204 of one or both of the local device 102 and/or remote device 104, in response to the exchange of the authentication information, may determine whether the authentication policy of device 102 or device 104 controls which device must authenticate first. In particular, authentication engine 204 in one or more of the devices 102, 104 compares the authentication information to determine whether one of the devices has a higher authentication priority and/or device class.

[0029] According to one embodiment, if the authentication information from the two devices share a common authentication priority, authentication agent 204 in the devices may break the "tie" through analysis of the device significance indicators.

EXAMPLE APPLICATION AND IMPLEMENTATION

[0030] An example implementation of the foregoing method is described herein are further illustrated with reference to the communication flow diagrams of Figs. 4-6, below. In particular, the following communication flow diagrams illustrate three alternate scenarios in accordance with an example WMAN implementation. In the first scenario (Fig. 4), each of the local device 102 (e.g., subscriber station) and the remote device 104 (e.g., base station) share the same authentication priority level. In the second scenario, (Fig. 5), the local device 102 has a higher authentication priority. The third scenario (Fig. 6) is representative of a situation in which the local device 102 is willing to initiate authentication regardless of the authentication priority of the remote device 104.

[0031] With reference to **Fig. 4,** a communication flow diagram exhibiting a method for determining authentication priority according to one example embodiment. As introduced above, the communication flow diagram of Fig. 4 is representative of a situation in which each of the devices 102, 104 share a common authentication policy, i.e., the authentication policy of both devices requires the other device to initiate authentication (i.e., disclosing its identity first).

[0032] As shown, the process of Fig. 4 begins with generation and issuance of message 402 including at least a subset of an authentication policy associated with the issuing device. According to one embodiment, the subset of the authentication policy includes authentication information such as, for example, one or more of authentication priority level and/or device class

information. According to one example embodiment, the issuing device is the subscriber station 102 in anticipation of authentication with a base station 104.

[0033] Upon receipt of message 402, a security agent 114 in the remote device(s) 104 respond with message 404 including at least a subset of an authentication policy associated with the remote device 104. As above, the message may contain authentication information including one or more of authentication priority level and/or device class information associated with the remote device, e.g., 104.

[0034] Upon receipt of at least a subset of authentication policy from remote device 104, security agent 112 invokes an instance of authentication engine 204 to compare authentication information received from the remote device 104 against authentication information contain in a local authentication policy. In particular, authentication engine 204 compares the authentication priority level of the remote device 104 against that of the local device 102. Security agent 114 in the remote device 104 similarly invokes authentication engine 204 to independently perform this analysis and identify which of the devices enjoys authentication priority. In accordance with this example scenario, they are both the same (e.g., "0") each requiring the other device to initiate the authentication. According to one example embodiment, the process may terminate at this point without subsequent authentication proceedings – i.e., an impasse.

[0035] In an alternate embodiment (denoted by dashed lines), introduced above, rather than succumbing to the apparent impasse, the authentication engine 204 in security agent 112, 114 may then compare the device class indication of the remote device against the local device to resolve the conflict. In this case, the security agents 112, 114 determine that local device 102 enjoys authentication priority based, a least in part, on a superior device classification, and the remote device initiates authentication proceedings with one or more messages 406. Once the

remote device 104 is authenticated to the local device 104, local device 104 completes the mutual authentication by issuing one or more authentication messages 408.

[0036] **Fig. 5** is a communication flow diagram exhibiting a method for determining authentication priority according to one example embodiment. More particularly, as introduced above, Fig. 5 represents a situation in which the local device 102 enjoys a higher authentication priority level over the remote device 104, requiring the remote device to initiate authentication proceedings (authenticating itself to the local device 102, before the local device authenticates to the remote device 104.

[0037] Briefly, as above, local device 102 generates and issues a message 502 to remote device 104 including at least a subset of an authentication policy associated with the local device 102. The subset of the authentication policy may include one or more of a authentication priority level and/or device class information. In this example, a security agent 114 in device 104 invokes an instance of authentication engine 204 to analyze the subset of the authentication policy embedded within the received message and determines that device 102 enjoys authentication priority over device 104. Accordingly, device 104 initiates authentication message(s) 504 before device 102 then completes the mutual authentication with message(s) 506.

[0038] **Fig. 6** is a communication flow diagram exhibiting a method for determining authentication priority according to one example embodiment.

[0039] More particularly, as introduced above, Fig. 6 represents a situation in which the local device 102 does not require a remote device to initiate authentication. In this case, local device 102 may generate and issue a message 602 including at least a subset of an authentication policy 212 prior to initiating authentication, but need not do so. That is, since the authentication policy 212 of device 102 does not require prior authentication of the remote device 104, local device

102 may simply initiate authentication on its own accord, denoted by messages 604. Upon (or in parallel with) authentication of device 102 to device 104, device 104 generates and issues message(s) 606 to complete the mutual authentication of device 104 to device 102, as shown.

Alternate Embodiment(s)

[0040] **Fig. 7** illustrates a block diagram of an example storage medium comprising content which, when accessed, causes an electronic appliance to implement one or more aspects of the security agent 200 and/or associated methods 300-600. In this regard, storage medium 700 includes content 702 (e.g., instructions, data, or any combination thereof) which, when executed, causes the appliance to implement one or more aspects of security agent 200, described above.

[0041] The machine-readable (storage) medium 700 may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs, and magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnet or optical cards, flash memory, or other type of media / machine-readable medium suitable for storing electronic instructions. Moreover, the present invention may also be downloaded as a computer program product, wherein the program may be transferred from a remote computer to a requesting computer by way of data signals embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem, radio or network connection).

[0042] In the description above, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without some of these specific details. In other instances, well-known structures and devices are shown in block diagram form.

[0043] Embodiments of the present invention may be used in a variety of applications. Although the present invention is not limited in this respect, the circuits disclosed herein may be used in microcontrollers, general-purpose microprocessors, Digital Signal Processors (DSPs), Reduced Instruction-Set Computing (RISC), Complex Instruction-Set Computing (CISC), among other electronic components. However, it should be understood that the scope of the present invention is not limited to these examples.

[0044] Embodiments of the present invention may also be included in integrated circuit blocks referred to as core memory, cache memory, or other types of memory that store electronic instructions to be executed by the microprocessor or store data that may be used in arithmetic operations. In general, an embodiment using multistage domino logic in accordance with the claimed subject matter may provide a benefit to microprocessors, and in particular, may be incorporated into an address decoder for a memory device. Note that the embodiments may be integrated into radio systems or hand-held portable devices, especially when devices depend on reduced power consumption. Thus, laptop computers, cellular radiotelephone communication systems, two-way radio communication systems, one-way pagers, two-way pagers, personal communication systems (PCS), personal digital assistants (PDA's), cameras and other products are intended to be included within the scope of the present invention.

[0045] The present invention includes various operations. The operations of the present invention may be performed by hardware components, or may be embodied in machine-executable content (e.g., instructions), which may be used to cause a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the operations. Alternatively, the operations may be performed by a combination of hardware and software. Moreover, although the invention has been described in the context of a computing appliance,

those skilled in the art will appreciate that such functionality may well be embodied in any of number of alternate embodiments such as, for example, integrated within a communication appliance (e.g., a cellular telephone).

[0046] Many of the methods are described in their most basic form but operations can be added to or deleted from any of the methods and information can be added or subtracted from any of the described messages without departing from the basic scope of the present invention. Any number of variations of the inventive concept are anticipated within the scope and spirit of the present invention. In this regard, the particular illustrated example embodiments are not provided to limit the invention but merely to illustrate it. Thus, the scope of the present invention is not to be determined by the specific examples provided above but only by the plain language of the following claims.